

УДК 520.607

Использование методов глубокого обучения для предсказания кибератак на основе анализа сетевого трафика

Севастей Егор Александрович

egor4sev@mail.ru

МГТУ им. Н.Э. Баумана, Москва, Россия

Аннотация. Рассмотрены отечественные патентованные методы предобработки сетевого трафика (фильтрация, нормализация, агрегация, кодирование), используемые для повышения эффективности нейросетевых моделей в задачах предсказания кибератак. Представлены алгоритмы машинного обучения (кластеризация, поведенческий анализ, графовые модели) и методы глубокого обучения (автоэнкодеры, CNN, LSTM, GNN), реализованные в отечественных разработках. Показано, что сочетание фрактального анализа, графовых представлений и гибридных архитектур обеспечивает повышение точности и устойчивости к шифрованию. Сделан вывод о перспективности применения гибридных нейросетевых систем в составе российских решений информационной безопасности.

Ключевые слова: кибератаки, глубокое обучение, сетевой трафик, предобработка данных, фрактальный анализ, нейросети

Введение. Современные системы кибербезопасности сталкиваются с ростом числа атак и усложнением их структуры. Традиционные сигнатурные методы не обеспечивают достаточного уровня защиты, что делает актуальным применение методов машинного и глубокого обучения. В отечественной практике разработан ряд патентов, направленных на фильтрацию, нормализацию и кодирование сетевого трафика, что формирует базу для эффективного обучения нейросетевых моделей [1, 2].

Методы и материалы; результаты. Проведен анализ патентов и отечественных решений: межсетевых экранов с мандатной фильтрацией (НПО «Эшелон»), систем корреляции распределенных событий (ИнфоТеКС), поведенческого анализа (Positive Technologies), а также методов выявления аномалий на основе фрактальных характеристик трафика [3, 4]. Рассмотрены архитектуры глубокого обучения: CNN для извлечения локальных паттернов, LSTM для анализа временных зависимостей, GNN для моделирования сетевых структур, автоэнкодеры для выявления zero-day атак. Установлено, что гибридизация статистических и нейросетевых методов обеспечивает высокую чувствительность к аномалиям и применимость в системах IDS/IPS и SIEM.

Заключение. Отечественные патентованные решения демонстрируют практическую реализуемость интеллектуальных подходов к анализу сетевого трафика. Предобработка (фильтрация, нормализация, агрегация) формирует качественные данные для обучения, а гибридные нейросетевые архитектуры позволяют предсказывать атаки на ранних стадиях. Полученные результаты

могут быть использованы при проектировании отечественных интеллектуальных систем обнаружения атак и модулей UEBA в составе SOC002E.

Список источников

- [1] Голяков В.А., Трусов С.С. *Методы и средства защиты компьютерной информации*. Москва, Форум, 2020, 416 с.
- [2] Хачумов И.В., Руденко В.А. *Анализ и обработка сетевого трафика: технологии, методы, средства*. Москва, Горячая линия — Телеком, 2019, 312 с.
- [3] Марков А.С. и др. *Межсетевой экран с фильтрацией трафика по мандатным меткам*. Патент № RU159041U1 РФ. НПО «Эшелон», 2023.
- [4] Репин Д.С. и др. *Способ обнаружения сетевых атак на основе фрактальных признаков*. Патент № RU2713759C1 РФ. ИнфоТеК, 2020.